Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : -
CIA-RDP90-00530R000500970003-3

[COMMITTEE PRINT]

4

SECURITY CLEARANCE PROCEDURES IN THE INTELLIGENCE AGENCIES

STAFF REPORT

SUBCOMMITTEE ON OVERSIGHT

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 1979

U.S. GOVERNMENT PRINTING OFFICE

51-417 WASHINGTON : 1979

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 :
CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

(Established by H. Res. 658, 95th Congress, 1st session)

EDWARD P. BOLAND, Massachusetts, *Chairman*

CLEMENT J. ZABLOCKI, Wisconsin
BILL D. BURLISON, Missouri
MORGAN F. MURPHY, Illinois
LES ASPIN, Wisconsin
CHARLES ROSE, North Carolina
ROMANO L. MAZZOLI, Kentucky
NORMAN Y. MINETA, California
WYCHE FOWLER, JR., Georgia

J. KENNETH ROBINSON, Virginia
JOHN M. ASHBROOK, Ohio
ROBERT McCLORY, Illinois
G. WILLIAM WHITEHURST, Virginia
C. W. BILL YOUNG, Florida

THOMAS K. LATIMER, *Staff Director*
MICHAEL J. O'NEIL, *Chief Counsel*
PATRICK G. LONG, *Associate Counsel*
JEANNE M. MCNALLY, *Clerk*

SUBCOMMITTEE ON OVERSIGHT

LES ASPIN, Wisconsin, *Chairman*

CHARLES ROSE, North Carolina
ROMANO L. MAZZOLI, Kentucky
EDWARD P. BOLAND, Massachusetts

JOHN M. ASHBROOK, Ohio
C. W. BILL YOUNG, Florida

LEON S. FUERTH, *Professional Staff Member*
RICHARD D. ANDERSON, Jr., *Professional Staff Member*
G. ELIZABETH KEYES, *Professional Staff Member*
PATRICIA GARBER, *Secretary*

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

CONTENTS

	Page
Introduction	1
Authorities, Procedures and Organization	3
Central Intelligence Agency	4
Department of State	6
Department of Defense	8
National Security Agency	11
Defense Intelligence Agency	12
Problems and Recommendations	13

CHARTS

I—State Department—Statistics on SCI Clearances	8
II—Department of Defense—Statistics on SCI Clearances	13
III—National Security Agency—Statistics on SCI Clearances	13
IV—Summary of the Similarities and Differences for Gaining SCI Access in the Intelligence Community	14

APPENDIX

APPENDIX A–Executive Order 10450	21
APPENDIX B–DCID 1/14	25
APPENDIX C–Public Law 88–290	30
APPENDIX D–Testimony by the FBI concerning domestic security investigations	32

LIST OF WITNESSES

WEDNESDAY, MAY 16, 1979

Karl D. Ackerman, Deputy Assistant Secretary for Security, Department of State.
Robert Gambino, Director, Office of Security, Central Intelligence Agency.

THURSDAY, MAY 17, 1979

Thomas J. O'Brien, Director for Security Plans and Programs, Office of the Deputy Under Secretary of Defense for Policy Review, Department of Defense.
Col. Karl V. Haendle, Assistant Deputy Director for Security Services, Defense Intelligence Agency.
Arthur Mathisen, Assistant Deputy Director for Management Services, National Security Agency.

THURSDAY, MAY 24, 1979

Gordon H. Barland, Ph. D., American Polygraph Association.
Jeremiah S. Gutman, New York attorney, representing the American Civil Liberties Union.
Jack Blake, recently retired Acting Deputy Director of the Central Intelligence Agency.
Ray Cline, Executive Director, World Power Studies at Center for Strategic and International Studies.

THURSDAY, JUNE 21, 1979

Daniel P. Jaffe, Assistant Attorney General, Department of the Attorney General, Commonwealth of Massachusetts.
Thomas J. O'Brien, Director for Security Plans and Programs, Office of the Deputy Under Secretary of Defense for Policy Review, Department of Defense.
Bernard J. O'Donnell, Director, Defense Investigative Service, Department of Defense.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Harry W. Bratt, Director, National Criminal Justice Information and Statistics Service, Law Enforcement Assistance Administration, Department of Justice.
Helen Lessin, Office of General Counsel, LEAA, Department of Justice.
Carol Kaplan, National Criminal Justice Information and Statistics Service, Department of Justice.
Donald T. Perrine, Assistant Section Chief, Document Classification and Review Section, Records Management Division, Federal Bureau of Investigation.
Gary Stoops, Loyalty and Applicants Section, Federal Bureau of Investigation.
Lawrence Lawler, Section Chief, National Criminal Information Section, Federal Bureau of Investigation.
Conrad Banner, Deputy Assistant Director, Identification Section, Federal Bureau of Investigation.
Paul Nugent, Terrorism Section, Federal Bureau of Investigation.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

INTRODUCTION

The Oversight Subcommittee of the House Permanent Select Committee on Intelligence has recently completed an in-depth study of security clearance procedures used by the Central Intelligence Agency, the National Security Agency, the Department of State, and the Department of Defense. This effort was specially focused on procedures used to screen applicants for access to Sensitive Compartmented Information (SCI)—a particularly delicate and important category of intelligence data.

The subcommittee's interest in this area grew out of the recent proliferation of unathorized disclosures and incidents of espionage, involving members of the intelligence community or persons who were otherwise authorized access to intelligence information. Given the failure of the clearance and screening process to work in such well-publicized instances as the case of William Kampiles,[1] the subcommittee believed it would be useful to examine the system and to determine whether it is working effectively.

The obvious bottom line of any personnel security system is that it must be able to support reasonable determinations that hiring persons for intelligence work, or granting employees of the Federal Government (or its contractors) access to SCI is consistent with the national security. Based on the results of its investigation, the subcommittee believes that the screening process cannot presently meet uniform high standards in this regard. The subcommittee notes a number of factors which contribute to this conclusion:

Although the Director of Central Intelligence (DCI) is in theory (and in law) generally responsible for protecting intelligence sources and methods, this function is in fact diffused among a number of agencies.

Clearance procedures and philosophies differ widely among, and sometimes even within these agencies. There are, for example, major variations in the use of and attitudes towards the polygraph.

Cuts in manpower have placed pressure on investigative procedure and standards, and put a premium on efficient procedure and organization.[2]

Investigative branches report increasing difficulty in compiling adequate data bases from the FBI and other sources. A major problem appears to be inadequate access to criminal justice records.

---

[1] Kampiles, a former employee of the CIA, was convicted of espionage in 1978 for selling a classified document to the Soviets.

[2] DoD alone processed more than 100,000 persons for clearance last year. It should be noted that literally thousands of SCI clearances are held by employees of nonintelligence agencies. Although the subcommittee has not yet pursued this area, we do know that CIA and NSA account for the granting of about 2,500 of these. (Still other nonintelligence agencies grant their own SCI clearances. The Department of Justice for example grants SCI access and notifies the DCI after the fact.)

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

AUTHORITIES, PROCEDURES AND ORGANIZATION

SECTION I: THE FRAMEWORK OF LAWS AND REGULATIONS

The Director of Central Intelligence (DCI) is authorized to conduct background investigations of prospective and current employees of the CIA by the National Security Act of 1947 and the CIA Act of 1949. Both acts prescribe the establishment of programs and procedures for the protection of national security sources, methods and data.

Concern over revelations of Communist penetration of the U.S. Government in the late 1940's and early 1950's led to the publication of Executive Order 10450 [2a] (April 27, 1953) which established a security investigation program for the entire government. Executive Order 10450 remains the basis for security background investigations of government employees. The criteria and standards established in that Executive Order are still adhered to by all government agencies.

Executive Order 12036 (January 24, 1978) directs that

> The CIA shall protect the security of its installations, activities, information and personnel by appropriate means including such investigations of applicants, employees, contractors and other persons with similar associations with the CIA as are necessary. (1.811)

Executive Order 12036 also spells out the DCI's broader responsibility for setting clearance standards for the entire intelligence community.[3] Within this framework, the DCI has defined specific requirements that must be satisfied before access should be granted to SCI. These can be found in the Director of Central Intelligence Directive (DCID) 1/14 [4] which sets forth "minimum personnel security standards and procedures governing eligibility for access to Sensitive Compartmented Information (SCI)."

On the other hand, however, Executive Order 12036 also provides that

> All Foreign Intelligence Agencies (CIA, NSA, DIA, etc.) are authorized to conduct their own investigations of present, former or prospective employees as deemed necessary in the interest of national security (2.208(c)).

Given this latitude, each intelligence agency therefore maintains its own program for investigation, clearance and employment. In addition, a number of other departments and agencies conduct background investigations under Executive Order 10450; for example, the Office of Personnel Management (formerly the Civil Service Commission), the State Department and the Defense Department. The major screening programs are discussed below.

[2a] See appendix A.

[3] The DCI shall "Ensure the establishment by the Intelligence Community, of common security and access standards for managing and handling foreign intelligence systems, information and products." (1.601 (i))

[4] See appendix B.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

CENTRAL INTELLIGENCE AGENCY

CIA's security clearance procedures appear to be the most comprehensive and stringent in the intelligence community.

Once a detailed personal history statement has been filed, a full field background investigation of each applicant begins, based on the criteria established in Executive Order 10450 and DCID 1/14. According to the testimony of Robert Gambino, Director of Security at CIA, the purpose of this background investigation is to establish the applicant's identity and to determine that he or she is of unquestionable loyalty, excellent character, integrity, discretion and trustworthiness.[5]

A National Agency Check (NAC) is the first step of the full field background investigation. The NAC consists of a review of holdings which may be on file at the following federal agencies:

The Federal Bureau of Investigation;

The Office of Personnel Management ((OMP), formerly Civil Service Commission);

The Defense Central Indices of Investigation; and Coast Guard Intelligence, Department of Transportation, if the applicant has served in the military;

The Immigration and Naturalization Service (INS), if the applicant is an alien immigrant;

The State Department's passport files, to cover foreign travel; and other federal agencies as appropriate.

When the NAC uncovers a problem, CIA's Office of Security summons an applicant for a personal interview. Such interviews are not routine; they take place only if the NAC indicates that an applicant may have a problem meeting CIA security standards.

CIA's background investigation encompasses the last 15 years of an applicant's life or the years from his 17th birthday, whichever period is shorter. Identity is established through birth records, verification of parentage and citizenship. Investigators examine the applicant's education, employment, and residences and conduct neighborhood checks, criminal justice information checks and credit checks. A minimum of five character references must be interviewed with a view toward establishing the habits, loyalty and morals of the individual. Both positive and negative information must be taken into account

Material from the background investigation in the field is passed to CIA "appraisers" for evaluation. CIA's appraisal process categorizes problems under two headings: suitability and security. Suitability problems are processed by CIA's Applicant Review Panel (ARP), comprising 4 members: one from the Office of Personnel, one from the Office of Security, one from the Office of Medical Services and one from the Equal Employment Opportunity Office. Each panel member reviews a case individually and offers a separate evaluation to the Director of Personnel. Final decision on whether to accept or reject an applicant on suitability grounds is exercised by the Director of Personnel.

Security problems, on the other hand, are dealt with through an "adjudicative process". Should an appraiser's recommendation be negative on security grounds, the case is referred through a chain of experienced senior security officers. If their recommendation is negative, the case then goes to the Director of Security, who alone can

[5] "Security Clearance Procedures", Transcript, May 16, 1979.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

disapprove an applicant on security grounds. (The DCI has delegated this power to the Director of Security; however, the DCI maintains the power to overrule any decision made at that level.)

There are several suitability and security factors which would cause the automatic disqualification of an applicant. According to Mr. Gambino's testimony,[6] the following might be reasons for rejection on grounds of suitability: (1) emotional instability and immaturity; (2) personality idiosyncracies; (3) limited mental capacity/scholarship deficiencies; (4) physical impairments; (5) limitations precluding adapability and flexibility; (6) poor employment record; (7) financial irresponsibility; (8) alcohol abuse; and (9) marital difficulties.

The following would be considered disqualifying data in the security area: (1) illegal use of drugs; (2) thievery; (3) homosexuality; and (4) gross character deficiencies. Any characteristic clearly outside the criteria established by Executive Order 10450 or DCID 1/14 is sufficient reason for immediate rejection of any applicant case.

If no problems arise in the background investigation, or if adjudication has resolved any uncertainty, the applicant next submits to a physical exam and psychiatric screening. The psychiatric screening consists of a battery of tests designed to measure the candidate's professional flexibility, stress level, and reactions to pressure in the hope of identifying problems he or she might have as an employee of the Agency.[7] If there is an indication of abnormality, the candidate would be referred to a psychiatrist for an interview.

As the final step in the clearance process, all applicants for employment at the CIA are subject to a polygraph examination. CIA uses the polygraph to supplement and/or cross-check information developed by the background investigation. Questions asked during the examination are standard, with problem areas discussed beforehand. No set of questions is ever asked just once. Examiners look for repeated reactions; a single atypical reading cannot be used as evidence of lying or concealed problems. Control questions are used for comparison. During the exam, if the polygraph operator notes an abnormality, (repeated reaction to a particular area of inquiry), he will concentrate on this until it can be cleared up; there is no time limit on the exam.

Polygraph operators do not judge applicants; their function is to collect information and report it to apprasisers for evaluation. When security problems are revealed by the polygraph, the case must go back through CIA's adjudication process. Despite extensive use of the polygraph, CIA stresses that applicants are looked at from the "total person" standpoint, with the polygraph serving as an adjunct to this effort.

Ten percent (10 percent) of all CIA applicants are turned down for security reasons; 3 to 5 percent are turned down for suitability reasons. Of the ten percent (10 percent) security turndowns, twenty-four point five percent (24.5 percent) are turned down based on the background investigation alone; seventy-five percent (75 percent) are rejected on the basis of information derived from the polygraph, or the combination of polygraph results and the background investigation.[8]

---

[6] Ibid.

[7] CIA also uses psychological assessment designed to match the skills of the subject with particular assignments.

[8] It should be noted here, that because of the psychological effect the polygraph has on some of those being examined, a substantial number of revelations and admissions are volunteered prior to the actual testing. DoD and State, which do not use polygraph, believe that the same information can be obtained through a well-conducted personal interview without the aid of a polygraph. This raises the question, discussed below of whether the polygraph is in fact indispensable or merely one of several alternative screening tools.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

The polygraph can be waived for reasons of: inconclusive heart patterns, pregnancy, and physical disability. Waivers for other reasons must come from the DCI. If a subject refuses the exam on religious, moral or any other grounds, the polygrapher sends a statement with the reason to Security; polygraph examiners make no recommendation but report only the simple statement of fact. Admiral Turner recently granted two exceptions involving the polygraph: one for an applicant who took the polygraph but "did badly"; one for an applicant who refused the polygraph on moral grounds.

Every CIA employee is subject to reinvestigation at five year intervals. Reinvestigation consists of a neighborhood check, a police check, interviews with current and former supervisors and coworkers, and a polygraph. The polygraph questions at this time focus on counterintelligence issues. Repolygraphing is seen as a deterrent and as a way to detect security breaches.[9]

According to the CIA, when a "security allegation" or "special issue" involving an employee is raised, the polygraph clears people as often as it brings about an admission. Confession of a violation may lead to disciplinary action or termination of employment.

Finally, under CIA policy, contractors, military personnel and all people needing "staff-like access" [10] to the CIA go through the same clearance procedures as all other employees.

DEPARTMENT OF STATE

The Foreign Service Act of 1946 provides basic legal authority to establish procedures for determining the loyalty of Foreign Service Officer candidates. The State Department also draws authority for performing background investigations on prospective employees from Executive Order 10450, Executive Order 11652 and Executive Order 10865, all of which state that no person shall be given access to classified information and materials unless that person has been determined to be trustworthy and that his or her employment is clearly consistent with the national security.

After filing Standard Form 86 [11] (personal history statement), prospective employees are interviewed "in depth" by State Department security investigators. Investigators explain the standards which must be met to gain a clearance at the State Department. Questions are designed to be "deeply probing" so that the investigator may develop an understanding of the candidate. Interviewers first verify and clarify all information provided in the personal history statement. Applicants are then asked if there is anything in their background which, if revealed during the investigation, might conflict with the criteria for clearance. Interviewers aim to develop information to supplement the personal history statement, as an aid to a more accurate and thorough investigation.

---

[9] The subcommittee has determined that while CIA policy is, and has been, to reinvestigate employees every five years, such reinvestigations were for some time not conducted for the majority of employees, due to the pressure of other responsibilities on the staff of the Office of Security. In the wake of the Moore case, however, the five year requirement was again put into practical force. (Edwin Moore, a former employee of the CIA, was convicted of espionage in 1977, for attempting to transmit national defense information to the Soviets.)

[10] "staff-like access"—Term applied to persons needing unescorted entry to CIA's buildings in order to do their job.

[11] This is the Office of Personnel Management (OPM) standard application "Security Investigation Data for Sensitive Position":

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

The next step in the screening process is a medical examination. There is no pre-employment psychiatric screening or psychological assessment at State. After the medical, a full field background investigation begins. This investigation goes back 7 years or from an individual's 18th birthday, whichever period is shorter. State has its own security staff to conduct these investigations. There are approximately 450 professional level security agents in the State Department. However, in addition to security investigations, this staff is also charged with the protection of foreign diplomats.

The Department of State's approach to background investigations is on the principle that mere absence of disqualifying information is insufficient:

> There must be enough known positively about the indivudial * * * to conclude that he or she can be trusted with the responsibilities of more than routine consequence to the nation * * *. It is the purpose of the background investigation to acquire the information necessary and relevant to such a determination.[12]

Karl Ackerman, Deputy Assistant Secretary for Security at State, told the subcommittee that:

> Our investigative objective includes determining the individual's identity, establishing the continuity of his or her claimed background and activities, *and acquiring sufficient information to permit a reasonable conclusion to the individual's loyalty, character, integrity and trustworthiness.*[13] *(italic added).*

Most positions at State fall into what is known as the "critical-sensitive" category. The standard investigation for "critical-sensitive" positions at State is based on the criteria established in Executive Order 10450. For "critical-sensitive" positions, State believes that seven years' background is adequate. If, however, a SCI clearance is wanted, the investigation expands to cover the full fifteen-year minimum requirement of DCID 1/14. Both the standard investigation and the investigation for access to SCI are essentially the same except for the time element involved.

State's standard full field investigation consists of a National Agency Check (NAC), followed by verification of birth and citizenship. An applicant's education records will be checked if they fall within the seven year investigative period. If an applicant's education does not fall within the seven year period being checked, the highest level of education attained above high school must be verified. An applicant's employment for the last seven years is investigated, including an interview with the current employer. Any military service of a prospective employee is always checked whether or not it falls within the seven year investigative period. A minimum of four character references must be interviewed: two listed by the applicant and two developed by the investigator.

Neighborhood checks are used to verify the applicant's current address, as well as any other residences exceeding six months in duration over the last two years. Other addresses are verified when possible through education and employment checks. Both credit records and police records are investigated. State and Defense Department (see below) regard law enforcement records as their most productive and effective source of information. Both agencies note difficulties in gaining what they consider adequate access to criminal justice information.

---

[12] *Office of Security Instructions and Procedures*, Volume 2, "Investigations", (412.1) Department of State.
[13] "Security Clearance Procedures," transcript, May 16, 1979.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Information from the background investigation is compiled and sent to the Chief of the State Department's Evaluation Branch, where an analysis of the case is prepared and a recommendation is formulated. In the event of a negative recommendation on suitability grounds, the applicant's file is sent to State's Applicant Review Panel, comprising: the Chief of Evaluation, the Medical Advisor, and a member of the Office of Personnel. Most rejections at State are, in fact, on grounds of suitability rather than security. If enough adverse data is collected on an individual to warrant the case going before the Applicant Review Panel, the applicant is usually reinterviewed. Moreover, if the Applicant Review Panel recommends in favor of an applicant, but State's Office of Security disagrees, it will notify the Panel that although the subject is suitable he or she cannot be granted a security clearance, whereupon the case is closed. When a final negative decision is made, the applicant is informed in writing as to why employment and/or clearance has been denied. Where access to SCI is concerned, the Senior Intelligence Officer in State's Bureau of Intelligence and Research makes all final decisions. In calendar year (CY) 78, 746 SCI cases were adjudicated, of which three were denied.[14] There is no formal applicant appeal process.

Sensitive Compartmented clearances at State are revalidated at least every five years in a procedure which involves a review of the employee's security file, an internal name check and name checks with local authorities, and an update of biographic data. Revalidation does not involve reinvestigation unless information has been developed which requires follow-up. David McCabe, State Department Assistant Director for Personnel and Investigations, testified that there is no instance where revalidation has led State to cancel an SCI clearance.[15] If problems are discovered at this time or during the interim between initial employment and revalidation, the subject may be moved to a less sensitive position. Meanwhile, the employee may retain access to classified materials other than SCI.

The State Department makes only very limited use of the polygraph and does not use it as a preemployment screening device. State asserts that the procedure would be of little value for its purpose.

> Routine use of the polygraph is not essential to an effective clearance program and that * * * current procedures do, in fact, serve the personnel security needs of the Department well.[16]

CHART I

STATE—STATISTICS ON SCI CLEARANCES

	Adjudicated	Denied	Granted SCI	Revoked
Calendar year 1977	725	3	722	----------
Calendar year 1978	746	3	743	----------

DEPARTMENT OF DEFENSE

The Department of Defense has a centralized office to conduct its background investigations—the Defense Investigative Service (DIS).

[14] See Chart I.
[15] "Security Clearance Procedures," transcript, May 16, 1979.
[16] Additional remarks submitted for May 16, 1979 record, Department of State.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

DIS is authorized by DoD Directive 5105.42 to conduct preemployment personnel security investigations for the entire department. However, DIS, in turn, services a number of agencies[17] within DoD which all apply their own methods and procedures to determine whether or not to grant clearances.

DoD has three clearance categories: Sensitive Compartmented Information (SCI); Collateral/Top Secret; and Contractor/Confidential. Applicants for employment at DoD are cleared for specific kinds of intelligence access by investigative procedures varying according to the type of clearance. For SCI, the DIS conducts a Special Background Investigation (SBI); for Collateral/Top Secret, the DIS conducts a Background Investigation (BI).

Background Investigations, per DoD Directive 5210.8, cover the last five years of the applicant's life or from his 18th birthday, whichever is shorter. BI's are designed to lead to a determination that employment of a person is clearly consistent with national security. Successful completion and favorable adjudication permits an applicant to be cleared at the Collateral/TS level.

A BI includes a National Agency Check (NAC), verification of birth and citizenship, a check on college education and full time employment within the five year scope of the investigation, a check of local criminal justice records and, in the near future, will also include a credit check. BI's do not include neighborhood checks. However, the BI procedure requires DIS investigators to develop and personally interview three character references. These references must have sufficient knowledge of the applicant to comment intelligently on his background, suitability and loyalty. Foreign travel for more than 90 days within the investigation period is examined, and extensive inquiries are made when an applicant has foreign connections. If any negative information is developed during a Background Investigation, the BI must expand automatically to cover a full 15 years.

The Special Background Investigation (SBI) conforms to minimum investigative requirements prescribed by Executive Order 10450 and DCID 1/14. Successful completion and favorable adjudication result in a clearance for Sensitive Compartmented Information (SCI). SBI's cover the last 15 years of applicants' lives, including all those points needed for a BI. In addition, the SBI includes a neighborhood check and a credit check.

DIS requires verification of all residences for a period of 6 months or more during the past 5 years. The investigator tries to interview at least two neighbors who have enough knowledge of the applicant to comment on his suitability for a senstive position.

Credit bureau checks go back 5 years. When credit bureau records are not available, credit references must be interviewed. Points of concern are financial responsibility and/or any unexplained affluence.

Persons entering military service enlist for specific Military Occupational Specialities (MOS). After such persons have been interviewed for enlistment and tested for aptitude, they are given a security interview. At this point, approximately 60 percent of those who would be intellectually qualified for positions involving access to intelligence data are dismissed from further consideration. During

[17] This includes the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the Army, Navy and Air Force.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

basic training, candidates for security clearance file a Statement of Personal History (DD 398). A prenomination interview is held and the person is examined again from a security standpoint. This process eliminates another 12 percent. Special Background Investigations (SBI) begin at this point for those who have favorably completed processing.

DoD's screening process for civilians is much the same as for the military. Civilian applicants are first interviewed for employment qualifications, and are informed at this point that a background investigation will be needed. Applicants file Standard Form 171 and DD 398, Statement of Personal History, and then are called for a pre-employment security interview. The interview determines if there is any automatically disqualifying information about the applicant. Any information clearly outside the guidelines of DCID 1/14 eliminates the applicant for SCI but not necessarily for other types of clearance. It is exceptional for a person to be eliminated at this point; ordinarily the prenomination interview leads to an SBI.

Under Executive Order 10865, the Department of Defense administers an industrial security (i.e., contractors) program for DoD, its agencies (NSA, DIA), and 15 other departments and agencies of the government. When a contract requiring SCI clearance is to be awarded, DoD investigates the management and key officials of the company in question. Foreign ownership, control or influence will disqualify a company. If all is well, the contracting agency will instruct DIS to conduct an SBI based on Executive Order 10450 and DCID 1/14. There are approximately 13,000 SCI-cleared contractors currently associated with DoD, and there are 1.2 million contractor clearances of all kinds. For contractors who need Top Secret access, DIS will also do a background investigation; for Secret and Confidential access, a National Agency Check (NAC) is conducted. There is also a program of "company-confidential" clearances, whereby the contractor is authorized to grant employees access to confidential materials.

In 1974, the DIS suffered a 25 percent appropriations cut, causing a reduction in the DIS work force from 3,000 to 1,800 spaces. After further cuts, DIS now has approximately 1,000 positions with 860 agents in the field. These agents conducted 120,000 BI's in calendar year 1978.

Prior to 1974, DIS routinely covered a 15-year period for all background investigations. Because of its manpower losses, DIS now requires that only the Special Background Investigation for access to SCI must cover 15 years. Requirements for other clearances were reexamined, coverage diminished and reporting standards abridged. For example, under a "no news is good news" approach, favorable information about an individual is written up in very summary fashion; only negative data is developed and reported in detail.

Both DIA and NSA have criticized background information they are obtaining from DIS. Col. Carl V. Haendle of the DIA stated during testimony on May 17, that:

> From the standpoint of those who have to adjudicate investigations and make decisions as to whether an individual has access to Sensitive Compartmented Information, I am less than pleased with the information that we have to make that decision on.[18]

[18] Transcript, "Security Clearance Procedures", May 17, 1979.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Mr. Arthur Mathisen of the NSA expressed these same sentiments.

> If we are going to make affirmative findings regarding people that are very important in their lives and to the Agency, we really need data to put everything in context. We need information that is positive about reliability and trustworthiness and integrity, character, reputation. That is missing and makes the adjudication a difficult process to be fair.[19]

Shortcomings in DIS' performance were underscored in 1978, when it was learned that DIS had done the Special Background Investigation on an individual who had applied at DoD under an assumed identity. The SBI failed to detect this and the individual was cleared for SCI access. On another occasion, an Air Force enlistee was cleared for access to "Secret" inforation, although it was later learned he had been granted clearance under a false name. The Department of Defense has initiated meetings between the producers and consumers of DIS investigations. The subcommittee hopes that some of the issues highlighted during its hearings will be resolved, and looks forward to the outcome of these meetings.

THE NATIONAL SECURITY AGENCY

As a result of hearings held by the House UnAmerican Activities Committee in 1962, Congress enacted Public Law 88–290 [20] which provides specifically that employment of any person at the National Security Agency must be deemed in the interest of the national security.

Applicants at NSA are initially briefed on the criteria that must be satisfied for employment with the agency. They are advised that proof of citizenship, and information on membership in organizations, use of drugs, foreign travels and other overseas associations will be sought. The applicant then files DD 398, Personal History Statement.

The first step in NSA's clearance process is a polygraph examination. This procedure is based on DoD Directive 5210.48. It is worth noting however, that 5210.48 stipulates that

> The polygraph shall be employed only as an aid to support other investigative techniques and be utilized generally only after the investigation by other means has been as thorough as ciricumstances permit.[21]

The Directive goes on to state specifically that the polygraph may be used on "those competitive career employees of the Defense agencies who are to be assigned for training in * * * the National Security Agency." [22] Notwithstanding the prescribed sequence, NSA polygraphs prior to the background investigation as an initial security screening measure.

The principal difference between NSA and CIA polygraphing is that NSA explicitly uses the polygraph as a primary tool for the collection of adverse information. According to NSA, at least 95 percent of all negative information on applicants comes from the polygraph; 8590 percent of this information, in turn, is considered significant enough to warrant investigation. Out of 2,531 applicants for whom security processing was completed during fiscal year 1978, 775 were closed out by the Joint Personnel Security/Medical Review Panel

[19] Ibid.
[20] See Appendix C.
[21] DoD Directive 5210.48 "The Conduct of Polgraph Examinations and the Selection, Training and Supervision of DoD Polygraph Examiners." Sec. III–A.
[22] Ibid. Enclosure I, c, 1, b.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

without a favorable hiring determination. In roughly 90 percent (about 700) of these cases, the polygraph report was a contributing factor in the decision.[23]

NSA uses the polygraph screening technique only on its civilian applicants. Military assignees are exempted on the grounds that their assignment to duty at NSA is not voluntary. Since submission to a polygraph examination must be a voluntary act, NSA considers that requiring it of military personnel would violate their rights. In contrast, CIA polygraphs all military employees assigned to them, noting that their association with CIA is voluntary. It is an interesting question, whether this volutary/involuntary distinction is meaningful in the context of the all-volunteer military service.

A further peculiarity relating to military personnel at NSA is that when such persons retire and seek reemployment as civilians, they are then subject to the polygraph. Sixty-eight (68) military assignees found themselves in that position during fiscal year 1978. Approximately 20 percent of these candidates were adjudicated unfavorable by the Joint Personnel/Security/Medical Panel. In 90 percent of these cases, information obtained through the polygraph contributed to the decision. This means that thirteen (13) people who already had access to SCI through the clearance process at DoD were denied such access when NSA procedures came into play.

Following the polygraph, applicants undergo psychological testing. A psychological assessment battery is used as an aid in determining suitability and acceptability for employment at NSA and access to SCI. Ninety percent of all applicants are interviewed by a clinical psychologist. The results of the polygraph and the psychological tests are evaluated and information developed from them is forwarded to the Defense Investigative Service (DIS) for the Special Background Investigation (SBI).

SBI results are sent to NSA for evaluation. All information obtained about an applicant from the polygraph, psychological testing, and the full field investigation is then put together and brought before NSA's Applicant Review Panel (ARP). The ARP is comprised of representatives from NSA's Personnel, Medical and Security offices. It examines each applicant on the "total person" principle. The Panel either decides in favor of employment and access, or refers cases to NSA's Director of Personnel.

DEFENSE INTELLIGENCE AGENCY

The Defense Intelligence Agency (DIA) conducts its own adjudication after a personal interview, and a Special Background Investigation (SBI) is conducted by DIS.[24]

Col. Karl V. Haendle testified that in "the absence of any significant derogatory information, the decisions are made at the branch level to grant SCI access." [25] Where there is "significant derogatory information," cases are referred to a security review panel. The original adjudicator outlines the case and makes a recommendation. Cases are then reviewed by several senior security officials each of whom makes a

[23] The Committee notes, however, that NSA keeps no statistics record of the reasons why persons are denied employment. NSA records only reflect that a person was denied employment, but not whether a security issue was involved. See Chart III, Page 13.

[24] See Chart II, Page 13.

[25] Security Clearance Procedures. Transcript, May 17, 1979.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

recommendation. All these recommendations ultimately go to the Assistant Deputy Director for Security Services, DIA, for final determination.

DIA considers the following information to be automatically disqualifying: use of illegal drugs, financial irresponsibility, indebtedness, homosexuality, foreign relatives, immediate relatives foreign-born who have made no attempt to become U.S. citizens, and mental and emotional problems.

In contrast to CIA and NSA, DIA does not polygraph as part of its security screening process. Current policy provides for the polygraph to be used only to resolve situations which cannot be settled in any other way.

POST-EMPLOYMENT SECURITY ISSUES

After a person has been cleared and employed at DoD, if a security issue arises or adverse information about the person comes to the attention of a supervisor, an evaluation must be made. If there is reason to believe that such a person's activities constitute an immediate threat to the national security, emergency suspension of the subject's clearance occurs. If, after a detailed investigation, continuing the person's clearance is still not considered to be consistent with the national security, the clearance is removed.

Cases of espionage are referred to the Federal Bureau of Investigation for followup examination. Clearances in such instances are lifted at the time the case is referred, unless for the purpose of insuring a complete resolution of the case, the FBI requests that it not be.

CHART II

DEPARTMENT OF DEFENSE—STATISTICS ON SCI CLEARANCES

	Adjudicated	Denied	Granted SCI	Revoked
Army (April 1978 to March 1979)	[1] 10,500	[1] 710	9,790	232
Navy (calendar year 1978)	11,280	173	11,107	306
Air Force (calendar year 1978)	7,900	381	7,519	456
DIA (calendar year 1978)	5,985	48	5,937	35
Total			34,353	[2] 1,029

[1] Estimates.
[2] Or 3 percent.

CHART III

NATIONAL SECURITY AGENCY—STATISTICS ON SCI CLEARANCES

	Adjudicated	Denied	Processing not completed	Granted SCI	Revoked
NSA (fiscal year 1978)	2,531	[1] 775	732	1,024	14 (or 1.37 percent) civilian; 23 (or 2.25 percent) military.

[1] In 90 percent or 700 of these, information learned on the polygraph was a contributing factor.

PROBLEMS AND RECOMMENDATIONS

Broadly speaking, the subcommittee sees two overall areas where a need exists for improvements in the way security screening is carried out: there is a need for greater uniformity in investigative procedures

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

and standards; and there is a need for improved access to pertinent information.

PROCEDURES AND STANDARDS

DCID 1/14 established minimum security standards and procedures governing access to SCI. However, as the subcommittee has discovered, each agency conducts its own investigation, and all such investigations differ one from the other in depth, scope, and technique.

It is clear that each part of the intelligence community has peculiar needs, and that there is a role for diversity in the design and operation of personnel security systems. On the other hand, it also seems logical that to the extent each agency is trying to protect similar kinds of data—e.g., SCI—granting clearances ought to involve basically similar information about applicants, allowing for some reasonable variation.

The subcommittee believes, however, that, even making allowances for varying needs among intelligence agencies, the divergencies in their screening techniques have become excessive. Chart IV graphically illustrates how widely differentiated these procedures are.

CHART IV

[Key: ●—Yes; ○—No]

	CIA	State	DOD/DIA	NSA
Prenomination interview	●	●	●	●
Background investigation	●[1]	●	●	●[2]
Psychiatric screening	●[3]	○	○	●
Psychological assessment	●	○	○	●
Polygraph examination	●[4]	○	○	●[5]
Polygraph military personnel	●	○	○	○
All types data (positive and negative)	●	●	○	○
SCI clearance: A condition of employment	●	○	○	●

[1] Conducted prior to the polygraph exam.
[2] Conducted by DIS following the polygraph exam.
[3] Testing for professional flexibility, stress level and reactions to pressure. If there are problems, an interview by a psychiatrist follows.
[4] Administered after the background investigation on all civilian applicants and military personnel.
[5] Used prior to the background investigation for leads; is the primary source for negative information; used only on civilian applicants; military personnel are exempt.

Several features recorded on the chart merit further comment.

The subcommittee notes, for example, an existing pattern according to which persons being screened for the two most sensitive agencies of our government, the so-called intelligence "producers"—CIA and NSA—will not be granted employment unless they can be cleared for SCI from the start. On the other hand, employment by the so-called "intelligence consumers"—DoD and State—is not based on SCI access being granted. At DoD and State, a person can begin employment with access to other classified data, up to and including "Top Secret," and need only be cleared for SCI later upon need.

The label "Top Secret," however, is applied to information, "the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security." [26] The subcommittee believes that the boundary line between "Top Secret" and SCI information, in terms of pertinence to national security, is likely to be so thin that persons being cleared for "Top Secret" access ought to be subject to the same background investigation as those being cleared for SCI even if actual SCI access is not yet required.

[26] E.O. 12065 Section I-102.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

The subcommittee also notes a major discrepancy among the services in terms of the basic profile of information considered relevant to the clearance process. CIA and the Department of State, for example, stress the need—under the "whole person" concept—to search out both positive and negative information about candidates. The DIS, on the other hand, follows an approach which essentially downplays positive information and focuses overwhelmingly on a search for the negative. No news is not necessarily good news, however. While DIS' approach obviously helps it stretch manpower resources further, the subcommittee sees this technique as a point of weakness in the DIS product, and believes that in order for the screening process to be effective, both positive and negative data must be sought out and weighed.

As the chart shows, no feature of the security screening process is marked by greater interservice difference and by more anomalies than the polygraph.

CIA and NSA polygraph people whose intended level of access is so low—receptionists, char-force, et cetera—as to raise a question whether the investment is worthwhile. Other agencies hardly use the polygraph and argue that other techniques are equally effective for their purposes.

CIA uses the polygraph on all applicants, military and civilian, while NSA exempts military personnel. DIA, meanwhile, does not polygraph, although the agency is clearly involved in the production of SCI intelligence.

ILLEGIB

—CIA polygraphs as a last step, while NSA uses the polygraph as the first step in its screening process, although this appears to contradict the sense of DoD Directive 5210.48. Both agencies adhere to the "whole person" approach to clearance, but NSA's heavy reliance on the polygraph may be inconsistent with a well-balanced approach.

Evidence presented to the subcommittee demonstrates the that polygraph accounts for a substantial proportion of decisions to deny access. On the other hand, gaps in the statistics kept by the intelligence services do not make it possible to make the clear judgment that the polygraph is unique and indispensable. There has been insufficient research on the accuracy of the polygraph technique in screening job applicants. The subcommittee urges the DCI to conduct a study to validate the accuracy of the polygraph in the preemployment setting and to establish some level of confidence in the use of that technique.

The subcommittee also feels that the intelligence community should consider whether and how it can exercise more discrimination in the use of the polygraph. One basic constraint already in effect owes to the fact that the polygraph, by and large, is used in the so-called "intelligence-producing" services rather than in the "intelligence consuming" agencies. Although this concept is not embodied in any regulation, it may make sense insofar as it can simultaneously protect intelligence sources and methods, while establishing a reasonable outer limit to polygraphing. If this arrangement is to be truly secure, however, close attention must be paid to assure that as SCI moves through government, sources and methods are in fact kept under protection. The subcommittee understands that the DCI is studying methods for processing intelligence with this view. The Subcommittee may be interested in looking into this area at a later date.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

In light of these significant variations in practice regarding the polygraph, the subcommittee believes that the DCI, in consultation with the heads of other intelligence agencies and departments, should establish some communitywide criteria relating to the use of the polygraph. Once these criteria have been established, they should be absolute conditions of employment and waivers should only be granted by the heads of any of the intelligence agencies in extraordinary circumstances.

All these differences of technique underscore the fact that each program is administered by separate screening bureaucracies answering to several parent institutions.

Each of these screening systems faces a heavy case load complicated not only by uncertain legal standards and diminished public responsiveness, but by reductions in work force combined in some cases with a multiplication of responsibilities.

The DIS, for example, exhibits all these problems. As has been noted, DIS suffered a substantial reduction in force some years ago. Meanwhile, as the subcommittee learned in the course of its hearings, DIS investigators are also assigned to investigate white collar crime in the Department of Defense. A similar situation exists in the State Department, many of whose investigators double in brass, arranging for the protection of foreign dignitaries visiting the United States.

More uniform procedures seem to be needed, along with some means to assure quality control across the entire set of systems. It is possible, in fact—and the subcommittee believes the Executive Branch should examine the benefits and costs of such a proposal—that the solution to both the procedural and the resource problems is to establish a centralized office to conduct background investigations for the entire intelligence community. Such an office need not replace the adjudicative systems presently used by the intelligence services, but could, rather, provide these systems with a more standardized and qualitatively superior form of background information about candidates for employment or SCI access. Certainly, if such a body were to be established, the subcommittee believes that its sole function should be the conduct of security investigations. Other, unrelated activities of the types now burdening some of the services, can only be to the detriment of their main objectives.

ACCESS TO INFORMATION

The intelligence agencies have testified before the subcommittee that criminal justice records provide their most effective and productive source of leads for negative information developed by background investigations. The subcommittee has heard repeatedly, however, not only about the need for access to criminal justice records, but about the roadblocks involved.[27]

---

[27] Karl Ackerman, the Deputy Assistant Secretary for Security at the State Department, stated at the hearing on clearance procedures on May 16 that:

"* * * we have encountered more than a few cases doing routine police checks where the constraints as perceived in a given local jurisdiction by privacy legislation has caused them to question whether they are able to give us information from police check files. We have * * * run into the question of whether E.O. 10450 is indeed a proper statutory background for release of that information to us. Some (have) gone so far as to say, well, you know, if that were a law—they are really questioning, I suppose, whether the executive orders have the force of law. But it is being triggered by concerns for privacy." (p. 43)

The Director for Security Plans and Programs at Defense, Thomas J. O'Brien, expressed the same sentiments during testimony on May 17; O'Brien evaluating the investigation by the DIS, stated:

"* * * as far as the lessening of quality, I think an awful lot of it relates to that information that will be released by institutions, local law enforcement agencies * * * There seems to be much, much less of that, with the standard remark furnished by the DIS agent is that this particular jurisdiction will not provide that information."

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Problems in this area arise primarily from guidelines established by the Law Enforcement Assistance Administration (LEAA). LEAA defines "criminal history record information" as information collected by criminal justice agencies (courts, government agency or subunit thereof involved in the administration of criminal justice) on individuals "consisting of identifiable descriptions and notations of arrests, detentions, indictments, information or other criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release." [28]

These guidelines on Criminal Justice Information Systems place no restrictions whatsoever on the dissemination of conviction data, arrests made within the year of an inquiry, and arrests where charges are actively pending. However, the guidelines state specifically that policies regarding dissemination of nonconviction data by law enforcement agencies is left to states, and that is where the problem occurs.[29] Because LEAA guidelines allow all 50 states to develop their own policies on dissemination of criminal justice information to non-law enforcement agencies, a very scattered pattern exists. Much useful information is denied intelligence agency investigators.

To overcome this problem, federal legislation would be necessary. Such legislation could state that the intelligence agencies shall have access to the personal records of a subject, upon the subject's written consent, for the sole purpose of supplying information pertinent to the granting of a security clearance. The legislation might call not only for access to criminal justice records, but also education, employment, credit and medical records. As a safeguard, the law might require that this information be used only by intelligence services and disseminated to each other only for employment purposes.

Witnesses before the subcommittee also noted that certain information formerly available from the FBI in the course of an NAC is no longer obtainable—that is, information on groups which "advocate the use of force or violence to overthrow the government of the United States" or information on groups which "unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution." [30] The collection of such information was greatly curtailed by the institution of the Attorney General's Domestic Security Investigation Guidelines in June, 1976. The essence of those guidelines is to restrict investigations of individuals or groups advocating force or violence to overthrow the government or deprive others of their constitutional rights to those individuals or groups who may be engaged in activities which involve or will involve the use of force or violence and which involve a violation of federal law. It is this stricture that has led to the large scale reductions in domestic security investigations since 1976.[31]

The subcommittee recognizes that the purposes of the Domestic Security Investigation guidelines was, and is, to curtail investigation

---

[28] 28 CFR, "Judicial Administration", Subpart A, Section 20.3(b).

[29] State and local government wills determine the purpose for which dissemination of criminal history record information is authorized by State law, executive order, local ordinance, court rule, decision or order. (28 CFR, 20, 21 C3)

[30] Section 8(a) (4) and (5), E.O. 10450.

[31] For an evaluation of the impact of these guidelines, see November 9, 1977 GAO report entitled "FBI Domestic Intelligence Operations: An Uncertain Future," GGD-78-10. An earlier GAO report "FBI Domestic Intelligence Operations—Their Purpose and Scope: Issues That Need To Be Resolved", 2/24/76 GGD-76-50 had found that the many domestic security investigations previously in existence were unproductive and did not lead to positive results and "The Erosion of Law Enforcement Intelligence and its Impact on the Public Security" report of the Subcommittee on Criminal Laws and Procedures", Senate Judiciary Committee 1978.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

of activities protected by the First Amendment—however extreme or unorthodox—absent a showing of illegality or the imminence of illegality.

The subcommittee also recognizes that the FBI is responsible for preventing the commission of federal crimes, including acts of terrorism and similar acts of violence. Such crimes threaten the lives and "domestic tranquility" of the American people, who have every right to expect that the Federal Government's law enforcement arm will be given the necessary authority to provide that protection. The FBI has the additional investigative responsibility under the law to identify applicants who constitute security risks so as to prevent those securing sensitive government employment.

The attempt, as reflected in the guidelines, to achieve an appropriate balance between concerns for freedom of speech and association and the government's responsibility to provide information necessary to satisfy the security needs of federal agencies whose employees must satisfy minimum standards consistent with the national security, has produced some anomalies.

One such anomaly lies in the fact that an intelligence agency, in investigating an applicant for a security clearance, must rely on the FBI for any information concerning that person's activities to overthrow the government or deprive others of their constitutional rights or those of a group to which the individual belongs, while the Domestic Security Investigation Guidelines do not permit the FBI to investigate such a person or a group unless the person or group is connected with actual or imminent acts of violence in violation of Federal law. Since the FBI is likely to be the only source of information on groups identified by Executive Order 10450, intelligence agencies are unable to secure information that could assist them in making security assessments under the Executive Order, since by its terms the Executive Order only requires information about advocacy or association.

Examples of the above were cited to the subcommittee, during the hearing on June 21, 1979.

Thomas J. O'Brien, of the Department of Defense, testified about procedures used by that agency in identifying security risks. Mr. O'Brien responded to questions by Committee staff member Herbert Romerstein and testified as follows: [32]

Mr. ROMERSTEIN. Where would you get that kind of information (regarding groups that plan the overthrow of the government by force and violence or to deny others their constitutional rights by violence) normally? Is there another agency that would supply it if they had the data?

Mr. O'BRIEN. We would go to the Federal Bureau of Investigation and inquire as to their knowledge of the organization.

Mr. ROMERSTEIN. If a group such as one of those referred to in Executive Order 10450 publishes a plan to penetrate the armed forces, from whom would you expect to get the information so that you could take protective measures to prevent such people from coming in?

Mr. O'BRIEN. Our primary source of information of this type is the Federal Bureau of Investigation.

Donald Perrine and Paul Nugent testified on behalf of the Federal Bureau of Investigation in response to a series of questions by Congressman C. W. (Bill) Young. They testified as follows:

Mr. YOUNG. I want to talk about the organizational cases. It is my understanding that most of them have been closed since the Attorney General's guidelines were issued.

[32] Sections of the transcript are presented as appendix D.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Mr. NUGENT. The answer to your question is yes, that the majority of the cases, investigative cases which have been closed since the adoption of the guidelines in April 1976 have been due to the criteria established by the guidelines for investigation. They either did not meet that criteria or were closed for other reasons, but the vast majority of them have been closed for that reason.

Mr. YOUNG. Now, if a case on an organization has been closed, is the FBI still permitted to collect public type information relative to the group and its activities?

Mr. NUGENT. No, sir.

Mr. YOUNG. What about the case of, say, a newspaper article.

Are you permitted to collect that?

Mr. NUGENT. To peruse the newspaper and clip it? No. sir, that is not done at this point.

Mr. YOUNG. You say it is not done. Are you not permitted to do it?

Mr. NUGENT. I say based on the Department ruling and that one investigative case which was cited specifically by the Department, we would not do that, and do not do that.

Mr. YOUNG. Are you allowed to read it and remember it?

Mr. NUGENT. I would think that might be allowable in the private confines of one's home.

Mr. YOUNG. When was the case on the Progressive Labor Party closed?

Mr. NUGENT. The Progressive Labor Party case was closed in September 1976, September 20, 1976, to be exact.

Mr. YOUNG. Well, the Progressive Labor Party has publicly proclaimed that they intend to take power in the United States by using "armed struggle" and that they are engaged in a program of penetrating the Armed Forces.

This information appeared in the Progressive Labor Magazine, their own magazine that was published in the spring of 1978.

In a case like this where they themselves have made this declaration, can the FBI collect these public documents on a group like the Progressive Labor Party, despite the fact that the case has been closed?

Mr. NUGENT. Absolutely not.

Mr. YOUNG. If the United States Army sent you a name in a national agency check of someone who had recently joined the PLP, and had penetrated the Army, which is what they say they are going to do, would you have to answer no record?

Mr. NUGENT. Well, that is a hypothetical question, I realize, and to answer hypotheticals is rather difficult, but if that name were submitted today and that individual had joined such an organization last week, I would say that the possibilities of our coming up with that name in a name check situation would be practically remote.

Mr. YOUNG. Not because you weren't able to do it, but because you weren't permitted to, is that it?

Mr. NUGENT. Well, we just wouldn't have the currency of information with respect to that organization which has been closed now for 3 years. The membership of that particular group and any other would have changed two times in that period of three years, and we wouldn't have the identities of the membership.

Mr. YOUNG. There has been previous testimony before this committee that the FBI closed the case on the Maryland Ku Klux Klan shortly before Maryland State Police arrested a number of the leaders of the group in a plot to bomb churches, Jewish temples and the home of a Member of Congress.

If the State Police had not had Sergeant John Cook under cover in this violent group, they very likely would have been able to bring off this act of terrorism.

Now, if someone had joined the Maryland Klan after you closed that case, and had then applied for security clearance, would you have had any information to supply in a national agency check?

Mr. PERRINE. Probably not unless it came from other sources, another investigative service who may have forwarded it to our agency, but as an active investigation on the part of the FBI, as Mr. Nugent indicated, no.

This is not to say that if violent, illegal acts do occur, or are imminent, that the FBI could not investigate. Rather, before such acts occur, groups cannot be investigated for mere advocacy of violence.

The subcommittee recognizes that the inconsistency between Executive Order 10450 and the Domestic Security Investigation Guidelines is bound to produce similar examples. The subcommittee is divided as to whether it is the Executive Order or the Guidelines which

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

should be reassessed, but all members of the subcommittee agree that the inconsistencies of these two policy documents should be resolved so as to provide a clearer understanding of what information should be collected and made available for security clearance investigations. This reassessment should also examine the provisions of the Privacy Act and take into account the applicable Supreme Court decisions. The upcoming consideration of the recently proposed FBI charter will offer an appropriate opportunity to resolve these issues.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

APPENDIX A

EXECUTIVE ORDER 10450

SECURITY REQUIREMENTS FOR GOVERNMENT EMPLOYMENT

Whereas the interests of the national security require that all persons privileged to be employed in the departments and agencies of the Government, shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States; and

Whereas the American tradition that all persons should receive fair, impartial, and equitable treatment at the hands of the Government requires that all persons seeking the privilege of employment or privileged to be employed in the departments and agencies of the Government be adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies governing the employment and retention in employment of persons in the Federal service:

Now, therefore, by virtue of the authority vested in me by the Constitution and statutes of the United States, including section 1753 of the Revised Statutes of the United States (5 U.S.C. 631); the Civil Service Act of 1883 (22 Stat. 403; 5 U.S.C. 632, *et seq.*); section 9A of the act of August 2, 1939, 53 Stat. 1148 (5 U.S.C. 118j); and the act of August 26, 1950, 64 Stat. 476 (5 U.S.C. 22–1, *et seq.*), and as President of the United States, and deeming such action necessary in the best interests of the national security, it is hereby ordered as follows:

SECTION 1. In addition to the departments and agencies specified in the said act of August 26, 1950, and Executive Order No. 10237 [1] of April 26, 1951, the provisions of that act shall apply to all other departments and agencies of the Government.

SEC. 2. The head of each department and agency of the Government shall be responsible for establishing and maintaining within his department or agency an effective program to insure that the employment and retention in employment of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security.

SEC. 3. (a) The appointment of each civilian officer or employee in any department or agency of the Government shall be made subject to an investigation. The scope of the investigation shall be determined in the first instance according to the degree of adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security, but in no event shall the investigation include less than a national agency check (including a check of the fingerprint files of the Federal Bureau of Investigation), and written inquiries to appropriate local law-enforcement agencies, former employers and supervisors, references, and schools attended by the person under investigation: *Provided*, that upon request of the head of the department or agency concerned, the Civil Service Commission may, in its discretion, authorize such less investigation as may meet the requirements of the national security with respect to per-diem, intermittent, temporary, or seasonal employees, or aliens employed outside the United States. Should there develop at any stage of investigation information indicating that the employment of any such person may not be clearly consistent with the interests of the national security, there shall be conducted with respect to such persons a full field investigation, or such less investigation as shall be sufficient to enable the head of the department or agency concerned to determine whether retention of such person is clearly consistent with the interests of the national security.

(b) The head of any department or agency shall designate, or cause to be designated, any position within his department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security as a sensitive position. Any position so designated shall be filled or occupied only by a person with respect to whom a full field

[1] CFR, 1951 Supp., p. 430.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

investigation has been conducted: *Provided,* that a person occupying a sensitive position at the time it is designated as such may continue to occupy such position pending the completion of a full field investigation, subject to the other provisions of this order: *And provided further,* that in case of emergency a sensitive position may be filled for a limited period by a person with respect to whom a full field preappointment investigation has not been completed if the head of the department or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records of such department or agency.

SEC. 4. The head of each department and agency shall review, or cause to be reviewed, the cases of all civilian officers and employees with respect to whom there has been conducted a full field investigation under Executive Order No. 9835 [2] of March 21, 1947, and, after such further investigation as may be appropriate, shall re-adjudicate, or cause to be re-adjudicated, in accordance with the said act of August 26, 1950, such of those cases as have not been adjudicated under a security standard commensurate with that established under this order.

SEC. 5. Whenever there is developed or received by any department or agency information indicating that the retention in employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, such information shall be forwarded to the head of the employing department or agency or his representative, who, after such investigation as may be appropriate, shall review, or cause to be reviewed, and, where necessary, re-adjudicate, or cause to be re-adjudicated, in accordance with the said act of August 26, 1950, the case of such officer or employee.

SEC. 6. Should there develop at any stage of investigation information indicating that the employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, the head of the department or agency concerned or his representative shall immediately suspend the employment of the person involved if he deems such suspension necessary in the interests of the national security and, following such investigation and review as he deems necessary, the head of the department or agency concerned shall terminate the employment of such suspended officer or employee whenever he shall determine such termination necessary or advisable in the interests of the national security, in accordance with the said act of August 26, 1950.

SEC. 7. Any person whose employment is suspended or terminated under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950, or pursuant to the said Executive Order No. 9835 or any other security or loyalty program relating to officers or employees of the Government, shall not be restored to duty or reemployed in the same department or agency and shall not be reemployed in any other department or agency, unless the head of the department or agency concerned finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of the national security, which findings shall be made a part of the records of such department or agency: *Provided,* that no person whose employment has been terminated under such authority thereafter may be employed by any other department or agency except a determination by the Civil Service Commission that such person is eligible for such employment.

SEC. 8. (a) The investigations conducted pursuant to this order shall be designed to develop information as to whether the employment or retention in employment in the Federal service of the person being investigated is clearly consistent with the interests of the national security. Such information shall relate, but shall not be limited, to the following:

(1) Depending on the relation of the Government employment to the national security:

(i) Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.

(ii) Any deliberate misrepresentations, falsifications, or omissions of material facts.

(iii) Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, sexual perversion, or financial irresponsibility.

(iv) An adjudication of insanity; or treatment for serious mental or neurological disorder without satisfactory evidence of cure.

(v) Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause him to act contrary to the best interests of the national security.

---

[2] CFR, 1947 Supp.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

(2) Commission of any act of sabotage, espionage, treason, or sedition, or attempts thereat or preparation therefor, or conspiring with, or aiding or abetting another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

(3) Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the government of the United States or the alteration of the form of government of the United States by unconstitutional means.

(4) Advocacy of use of force or violence to overthrow the government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.

(5) Membership in, or affiliation or sympathetic association with, any foreign or domestic organization, association, movement, group, or combination of persons which is totalitarian, Fascist, Communist, or subversive, or which has adopted, or shows a policy of advocating or approving the commission of acts of force or violence to deny other persons their rights under the Constitution of the United States, or which seeks to alter the form of government of the United States by unconstitutional means.

(6) Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

(7) Performing or attempting to perform his duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

(b) The investigation of persons entering or employed in the competitive service shall primarily be the responsibility of the Civil Service Commission, except in cases in which the head of a department or agency assumes that responsibility pursuant to law or by agreement with the Commission. The Commission shall furnish a full investigative report to the department or agency concerned.

(c) The investigation of persons (including consultants, however employed), entering employment of, or employed by, the Government other than in the competitive service shall primarily be the responsibility of the employing department or agency. Departments and agencies without investigative facilities may use the investigative facilities of the Civil Service Commission, and other departments and agencies may use such facilities under agreement with the Commission.

(d) There shall be referred promptly to the Federal Bureau of Investigation all investigations being conducted by any other agencies which develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests of the national security, or information relating to any of the matters described in subdivisions (2) through (7) of subsection (a) of this section. In cases so referred to it, the Federal Bureau of Investigation shall make a full field investigation.

SEC. 9. (a) There shall be established and maintained in the Civil Service Commission a security-investigations index covering all persons as to whom security investigations have been conducted by any department or agency of the Government under this order. The central index established and maintained by the Commission under Executive Order No. 9835 of March 21, 1947, shall be made a part of the security-investigations index. The security-investigations index shall contain the name of each person investigated, adequate identifying information concerning each such person, and a reference to each department and agency which has conducted an investigation concerning the person involved or has suspended or terminated the employment of such person under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950.

(b) The heads of all departments and agencies shall furnish promptly to the Civil Service Commission information appropriate for the establishment and maintenance of the security-investigations index.

(c) The reports and other investigative material and information developed by investigations conducted pursuant to any statute, order, or program described in section 7 of this order shall remain the property of the investigative agencies conducting the investigations, but may, subject to considerations of the national security, be retained by the department or agency concerned. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given thereto except, with the consent of the investigative

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

agency concerned, to other departments and agencies conducting security programs under the authority granted by or in accordance with the said act of August 26, 1950, as may be required for the efficient conduct of Government business.

SEC. 10. Nothing in this order shall be construed as eliminating or modifying in any way the requirement for any investigation or any determination as to security which may be required by law.

SEC. 11. On and after the effective date of this order the Loyalty Review Board established by Executive Order No. 9835 of March 21, 1947, shall not accept agency findings for review, upon appeal or otherwise. Appeals pending before the Loyalty Review Board on such date shall be heard to final determination in accordance with the provisions of the said Executive Order No. 9835, as amended. Agency determinations favorable to the officer or employee concerned pending before the Loyalty Review Board on such date shall be acted upon by such Board, and whenever the Board is not in agreement with such favorable determination the case shall be remanded to the department or agency concerned for determination in accordance with the standards and procedures established pursuant to this order. Cases pending before the regional loyalty boards of the Civil Service Commission on which hearings have not been initiated on such date shall be referred to the department or agency concerned. Cases being heard by regional loyalty boards on such date shall be heard to conclusion, and the determination of the board shall be forwarded to the head of the department or agency concerned: *Provided*, that if no specific department or agency is involved, the case shall be dismissed without prejudice to the applicant. Investigations pending in the Federal Bureau of Investigation or the Civil Service Commission on such date shall be completed, and the reports thereon shall be made to the appropriate department or agency.

SEC. 12. Executive Order No. 9835 of March 21, 1947, as amended, is hereby revoked. For the purposes described in section 11 hereof the Loyalty Review Board and the regional loyalty boards of the Civil Service Commission shall continue to exist and function for a period of one hundred and twenty days from the effective date of this order, and the Department of Justice shall continue to furnish the information described in paragraph 3 of Part III of the said Executive Order No. 9835, but directly to the head of each department and agency.

SEC. 13. The Attorney General is requested to render to the heads of departments and agencies such advice as may be requisite to enable them to establish and maintain an appropriate employee-security program.

SEC. 14. (a) The Civil Service Commission, with the continuing advice and collaboration of representatives of such departments and agencies as the National Security Council may designate, shall make a continuing study of the manner in which this order is being implemented by the departments and agencies of the Government for the purpose of determining:

(1) Deficiencies in the department and agency security programs established under this order which are inconsistent with the interests of, or directly or indirectly weaken, the national security.

(2) Tendencies in such programs to deny to individual employees fair, impartial, and equitable treatment at the hands of the Government, or rights under the Constitution and laws of the United States or this order.

Information affecting any department or agency developed or received during the course of such continuing study shall be furnished immediately to the head of the department or agency concerned. The Civil Service Commission shall report to the National Security Council, at least semiannually, on the results of such study, and shall recommend means to correct any such deficiencies or tendencies.

(b) All departments and agencies of the Government are directed to cooperate with the Civil Service Commission to facilitate the accomplishment of the responsibilities assigned to it by subsection (a) of this section.

SEC. 15. This order shall become effective thirty days after the date hereof.

DWIGHT D. EISENHOWER.

THE WHITE HOUSE,
April 27, 1953.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

APPENDIX B

DCID No. 1/14 13 May 1976

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE No. 1/14 [1]

MINIMUM PERSONNEL SECURITY STANDARDS AND PROCEDURES GOVERNING ELIGIBILITY FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION

(Effective 13 May 1976)

Pursuant to the provisions of Executive Order 11905, Section 102 of the National Security Act of 1947 and National Security Council Directives, the following minimum personnel security standards, procedures and continuing security programs are hereby established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors and other individuals who require access to Sensitive Compartmented Information [2] (hereinafter referred to as SCI). The standards, procedures and programs established herein are minimum and the departments and agencies may establish such additional security steps as may be deemed necessary and appropriate to ensure that effective security is maintained.

Purpose

1. The purpose of this Directive is to enhance the security protection of SCI through the application of minimum security standards, procedures and continuing security programs, and to facilitate the security certification process among Government departments and agencies.

Applicability

2. The provisions of the Directive shall apply to all persons (other than elected officials of the United States Government, federal judges and those individuals for whom the DCI makes a specific exception) without regard to civilian or military status, form of employment, official rank or position or length of service.

3. Individuals who do not meet the minimum security criteria contained herein and who are, therefore, denied access to SCI shall not, solely, for this reason, be considered ineligible for access to other classified information. Individuals whose access to SCI has been authorized as an exception granted in accordance with paragraph 7 below, shall not, solely for that reason, be considered eligible for access to other classification information.

General

4. The granting of access to SCI shall be controlled under the strictest application of the "need-to-know" principle under procedures prescribed in the several existing authorities which govern access thereto, and in accordance with the personnel security standards and procedures set forth in this Directive. All persons accountable under the authority of this Directive and given access to information (SCI) containing sources or methods of intelligence shall, as a condition of obtaining access, sign an agreement that they will not disclose that information to persons not authorized to receive it.

Personnel Security Standards

5. Criteria for security approval of an individual on a need-to-know basis for access to SCI are as follows:

a. The individual shall be stable, of excellent character and discretion and of unquestioned loyalty to the United States.

---

[1] This directive supersedes DCID 1/14 approved 1 July 1968.

[2] The term "Sensitive Compartmented Information" as used in this Directive is intended to include all information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term does not include Restricted Data as defined in Section II, Public Laws 585, Atomic Energy Act of 1954, as amended.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

b. Except where there is a compelling need and a determination has been made by competent authority as described in paragraph 7 below that every reasonable assurance has been obtained that under the circumstances the security risk is negligible:

(1) Both the individual and the members of his or her immediate family shall be US citizens. For these purposes "immediate family" is defined as including the individual's spouse, parents, brothers, sisters and children.

(2) The members of the individual's immediate family and persons to whom he is bound by affection or obligation should neither be subject to physical, mental or other forms of duress by a foreign power, nor advocate the use of force or violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means.

6. In exceptional cases, the Senior Intelligence Officer (SIO) of the Intelligence Community organization, or his designee, may determine that it is necessary or advisable in the National interest to authorize access to SCI prior to completion of the fully prescribed investigation. In this situation such investigative checks as are immediately possible shall be made at once, and should include a personal interview by trained security or counterintelligence personnel. Access in such cases shall be strictly controlled, and the fully prescribed investigation and final evaluation shall be completed at the earliest practicable moment.

Exceptions

7. The exceptions to paragraph 5.b.(1)(2) above may be granted only by the SIO or his designee, unless such authority has been specifically delegated to the head of an office of organization as set forth in inter-departmental agreements. All exceptions granted will be common sense determinations based on all available information, and shall be recorded by the agency making the exception. In those cases in which the individual has lived outside of the United States for a substantial period of his life, a thorough assessment of the adequacy of the investigation in terms of fulfillment of the minimum investigative requirements, and judicious review of the information therein must be made before an exception is considered.

Investigative Requirements

8. The investigation conducted on an individual under consideration for access to SCI will be thorough and shall be designed to develop information as to whether the individual clearly meets the above Personnel Security Standards.

9. The investigation shall be accomplished through record checks and personal interviews of various sources by trained investigative personnel in order to establish affirmatively to the adjudicating agency complete continuity of identity to include birth, residences, education, employments and military service. Where the circumstances of a case indicate, the investigation shall exceed the basic requirements set out below to ensure that those responsible for adjudicating access eligibility have in their possession all the relevant facts available.

10. The individual shall furnish a signed personal history statement, fingerprints of a quality acceptable to the Federal Bureau of Investigation and a signed release, as necessary, authorizing custodians of police, credit, education and medical records, to provide record information to the investigative agency. Photographs of the individual shall also be obtained where additional corroboration of identity is required.

11. Minimum standards for the investigation are as follows:

a. Verification of date and place of birth and citizenship.

b. Check of the subversive and criminal files of the Federal Bureau of Investigation, including submission of fingerprint charts, and such other National agencies as are appropriate to the individual's background. An additional check of Immigration and Naturalization Service records shall be conducted on those members of the individual's immediate family who are United States citizens other than by birth or who are resident aliens.

c. A check of appropriate police records covering all areas where the individual has resided in the US throughout the most recent fifteen (15) years or since age eighteen, whichever is the shorter period.

d. Verification of the individual's financial status and credit habits through checks of appropriate credit institutions and interviews with knowledgeable sources covering the most recent five (5) years.

e. Interviews with neighbors in the vicinity of all the individual's residences in excess of six (6) months throughout the most recent five (5) year period. This coverage shall be expanded where the investigation suggests the existence of some questionable behavioral pattern.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

f. Confirmation of all employment during the past fifteen (15) years or since age eighteen, whichever is the shorter period but in any event the most recent two years. Personal interviews with supervisors and co-workers at places of employment covering the past ten (10) years shall be accomplished.

g. Verification of attendance at institutes of higher learning in all instances and at the last secondary school attended within the past fifteen (15) years. Attendance at secondary schools may be verified through qualified collateral sources. If attendance at educational institutions occurred within the most recent five (5) years, personal interviews with faculty members or other persons who were acquainted with the individual during his attendance shall be accomplished.

h. Review of appropriate military records.

i. Interviews with a sufficient number of knowledgeable acquaintances (a minimum of three developed during the course of the investigation) as necessary to provide a continuity to the extent practicable, of the individual's activities and behavioral patterns over the past fifteen years with particular emphasis on the most recent five years.

j. When employment, education or residence, has occurred overseas (except for periods of less than five (5) years for personnel on US Government assignment and less than ninety days for other purposes) during the past fifteen years or since age eighteen, a check of the records will be made at the Department of State and other appropriate agencies. Efforts shall be made to develop sources, generally in the United States, who knew the individual overseas in order to cover significant employment, education or residence and to attempt to determine if any lasting foreign contacts or connections were established during this period. However, in all cases where an individual has worked or lived outside of the US continuously for over five years, the investigation will be expanded to cover fully this period in his life through the use of such investigative assets and checks of record sources as may be available to the US Government in the foreign country(ies) in which the individual resided.

k. In those instances in which the individual has immediate family members or other persons with whom he is bonded by affection or obligation in any of the situations described in subparagraph 5.b.(2), above, the investigation will include an interview of the individual by trained security, investigative or counter-intelligence personnel to ascertain the facts as they may relate to the individual's access eligibility.

l. In all cases the individual's spouse shall at a minimum be checked through the subversive files of the Federal Bureau of Investigation and other National agencies as appropriate. When conditions indicate, additional investigations shall be conducted on the spouse of the individual and members of the immediate family to the extent necessary to permit a determination by the adjudicating agency that the provisions of paragraph 5, Personnel Security Standards, above, are met.

m. A personal interview of the individual will be conducted by trained security, investigative or counterintelligence personnel when necessary to resolve any significant adverse information and/or inconsistencies developed during the investigation.

12. Where a previous investigation has been conducted within the past five years which substantially meets the above minimum standards, it may serve as a basis for granting access approval provided a review of the personnel and security files does not reveal substantive changes in the individual's security eligibility. If a previous investigation does not substantially meet the minimum standards or if it is more than five years old, a current investigation shall be required but may be limited to that necessary to bring the individual's file up-to-date in accordance with the investigative requirements set forth in paragraph 11 above. Should new information be developed during the current investigation which bears unfavorably upon the individual's activities covered by the previous investigation, the current inquiries shall be expanded as necessary to develop full details of this new information.

13. Programs shall be instituted requiring the periodic reinvestigation of personnel provided access to SCI. These reinvestigations will be conducted on a five-year recurrent basis, but on a more frequent basis where the individual has shown some questionable behavioral pattern, his activities are otherwise suspect, or when deemed necessary by the SIO concerned.[3]

[3] In DoD, an SIO may request, with the approval of the Secretary of Defense or his designee, more frequent reinvestigations under special circumstances.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

14. The scope of reinvestigations shall be determined by the SIO concerned based on such considerations as the potential damage that might result from the individual's defection or willful compromise of SCI and the availability and probable effectiveness of other means to continually evaluate factors related to the individual's suitability for continued access. In all cases, the reinvestigation shall include, as a minimum, appropriate National agency checks, local agency (including overseas checks where appropriate), credit checks and a personal discussion with the individual by trained investigative, security or counterintellgence personnel when necessary to resolve significant adverse information or inconsistencies.

15. The evaluation of the information developed by investigation on an individual's loyalty and suitability shall be accomplished under the cognizance of the SIO concerned by analysts of broad knowledge, good judgment and wide experience in personnel security and/or counterintelligence. When all other information developed on an individual is favorable, a minor investigative requirement which has not been met should not preclude favorable adjudication. In all evaluations the protection of the national interest is paramount. Any doubt concerning personnel having access to SCI shall be resolved in favor of the national security. The ultimate determination of whether the granting of access is clearly consistent with the interests of national security shall be an overall common sense determination based on all available information.

Continuing Security Programs

16. In order to facilitate the attainment of the highest standard of personnel security and to augment both the access approval criteria and the investigative requirements established by this Directive, member departments and agencies shall institute continuing security programs for all individuals having access to SCI. In addition to security indoctrinations, these programs shall be tailored to create mutually supporting procedures under which no issue will escape notice or be left unresolved which brings into question an individual's loyalty and integrity or suggests the possibility of his being subject to undue influence or duress through foreign relationships or exploitable personal conduct. When an individual is assigned to perform sensitive compartmented work requiring access to SCI, the SIO for the department, agency or Government program to which the individual is assigned shall assume security supervision of that individual throughout the period of his assignment.

17. The continuing security programs shall include the followings:

a. Security education programs to ensure that individuals who are granted access to SCI are intially indoctrinated and periodically thereafter instructed as to its unique sensitivity and that they understand their personal responsibility for its protection. The individual should be instructed that the ultimate responsibility for maintaining eligibility for continued access to SCI rests with with the individual. Therefore, the individual is encouraged to seek a propriate guidance and assistance on any personal problem or situation which may have a possible bearing on his eligibility for continued access to SCI, and security counseling should be made available. These instructions should be conducted by individuals having extensive background and experience regarding the nature and special vulnerabilities of the particular type of compartmented information involved.

b. Security supervisory programs to ensure that supervisory personnel recognize and discharge their special responsibility in matters pertaining to the security of SCI, including the eligibility for SCI access. Such programs shall provide practical guidance as to indicators which may signal matters of security concern. Specific instructions concerning reporting procedures shall be disseminated to enable the appropriate authority to take timely corrective action to safeguard the security of the United States as well as to provide all necessary help to the indivuidal concerned to neutralize his vulnerability.

c. Security Review Programs to ensure that appropriate security authorities invariably receive and exchange, in a timely manner, all information bearing on the security posture of persons having access to sensitive information. Personnel history information shall be kept current. Security and related files shall be kept under continuing review.

18. Whenever adverse or derogatory information is discovered or inconsistencies arise which could impact upon an individual's security status, appropriate investigations shall be conducted on a timely basis. The investigation shall be of sufficient scope necessary to resolve the specific adverse or derogatory information, or inconsistency, in question so that a determination can be made as to whether the individual's continued utilization in activities requiring SCI is clearly consistent with the interests of the national security.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Effective Date

19. This Directive supersedes DCID 1/14, 1 July 1968. Existing directives,[4] regulations, agreements and such other references governing access to SCI as defined herein shall be revised accordingly.

GEORGE BUSH,
Director of Central Intelligence.

---

[4] These include pertinent provisions of the Clearance Standards and Investigation and Evaluation sections of the Communications Intelligence Security Regulations.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

APPENDIX C

National Security Agency—Personnel Security Procedures

PUBLIC LAW 88-290; 78 STAT. 168

An Act to amend the Internal Security Act of 1950.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That:

The Internal Security Act of 1950 is amended by adding at the end thereof the following new title:

Title III—Personnel Security Procedures in National Security Agency

"REGULATIONS FOR EMPLOYMENT SECURITY"

SEC. 301. Subject to the provisions of this title, the Secretary of Defense (hereafter in this title referred to as the 'Secretary') shall prescribe such regulations relating to continuing security procedures as he considers necessary to assure—

"(1) that no person shall be employed in, or detailed or assigned to, the National Security Agency (hereafter in this title referred to as the 'Agency'), or continue to be so employed, detailed, or assigned; and

"(2) that no person so employed, detailed, or assigned shall have access to any classified information;

unless such employment, detail, assignment, or access to classified information is clearly consistent with the national security.

"FULL FIELD INVESTIGATION AND APPRAISAL

"SEC. 302. (a) No person shall be employed in, or detailed or assigned to, the Agency unless he has been the subject of a full field investigation in connection with such employment, detail, or assignment, and is cleared for access to classified information in accordance with the provisions of this title; excepting that conditional employment without access to sensitive cryptologic information or material may be tendered any applicant, under such regulations as the Secretary may prescribe, pending the completion of such full field investigation: And provided further, That such full field investigation at the discretion of the Secretary need not be required in the case of persons assigned or detailed to the Agency who have a current security clearance for access to sensitive cryptologic information under equivalent standards of investigation and clearance. During any period of war declared by the Congress, or during any period when the Secretary determines that a national disaster exists, or in exceptional cases in which the Secretary (or his designee for such purpose) makes a determination in writing that his action is necessary or advisable in the national interest, he may authorize the employment of any person in, or the detail or assignment of any person to, the Agency, and may grant to any such person access to classified information, on a temporary basis, pending the completion of the full field investigation and the clearance for access to classified information required by this subsection, if the Secretary determines that such action is clearly consistent with the national security.

"(b) To assist the Secretary and the Director of the Agency in carrying out their personnel security responsibilities, one or more boards of appraisal of three members each, to be appointed by the Director of the Agency, shall be established in the Agency. Such a board shall appraise the loyalty and suitability of persons for access to classified information, in those cases in which the Director of the Agency determines that there is a doubt whether their access to that information would be clearly consistent with the national security, and shall submit a report and recommendation on each such a case. However, appraisal by such a board is not required before action may be taken under section 14 of the Act of June 27, 1944, chapter 287, as amended (5 U.S.C. 863), section 1 of the Act of August 26, 1950, chapter 803, as amended (5 U.S.C. 22-1), or any other similar provision of law. Each member of such a board shall be specially qualified and trained for his

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

duties as such a member, shall have been the subject of a full field investigation in connection with his appointment as such a member, and shall have been cleared by the Director for access to classified information at the time of his appointment as such a member. No person shall be cleared for access to classified information, contrary to the recommendations of any such board, unless the Secretary (or his designee for such purpose) shall make a determination in writing that such employment, detail, assignment, or access to classified information is in the national interest.

"TERMINATION OF EMPLOYMENT

"SEC. 303. (a) Notwithstanding section 14 of the Act of June 27, 1944, chapter 287, as amended (5 U.S.C. 863), section 1 of the Act of August 26, 1950, chapter 803, as amended (5 U.S.C. 22–1), or any other provision of law, the Secretary may terminate the employment of any officer or employee of the Agency whenever he considers that action to be in the interest of the United States, and he determines that the procedures prescribed in other provisions of law that authorize the termination of the employment of that officer or employee cannot be invoked consistently with the national security. Such a determination is final.

"(b) Termination of employment under this section shall not affect the right of the officer or employee involved to seek or accept employment with any other department or agency of the United States if he is declared eligible for such employment by the United States Civil Service Commission.

"(c) Notwithstanding section 133(d) of title 10, United States Code, any authority vested in the Secretary of Defense by subsection (a) may be delegated only to the Deputy Secretary of Defense or the Director of the National Security Agency, or both.

"DEFINITION OF CLASSIFIED INFORMATION

"SEC. 304. For the purposes of this section, the term 'classified information' means information which, for reasons of national security, is specifically designated by a United States Government agency for limited or restricted dissemination or distribution.

"NONAPPLICABILITY OF ADMINISTRATIVE PROCEDURE ACT

"SEC. 305. The Administrative Procedure Act, as amended (5 U.S.C. 1001 et seq.), shall not apply to the use or exercise of any authority granted by this title.

"AMENDMENTS

"SEC. 306. (a) The first sentence of section 2 of the Act of May 29, 1959 (50 U.S.C. 402 note), is amended by inserting, 'without regard to the civil service laws,' immediately after 'and to appoint thereto'.

"(b) Subsection (5) of section 2 of the Performance Rating Act of 1950 (5 U.S.C. 2001(b) is amended—

"(1) by striking out the period at the end of paragraph (13) and inserting in lieu thereof a semicolon; and

"(2) by adding at the end thereof the following new paragraph:

"'(14) The National Security Agency.'"

Approved March 26, 1964.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

APPENDIX D

To Oversight Report

Thomas J. O'Brien, of the Department of Defense, testified, on June 21, 1979, about procedures used by that agency in identifying security risks. Mr. O'Brien responded to a series of questions by Committee staff member Herbert Romerstein and testified as follows:

Mr. Romerstein. Among the criteria in Executive Order 10450 for denying employment are knowing membership in a group that plans the overthrow of the government by force and violence, or knowing membership in a group that advocates the use of violence to deny others their civil rights.

Does the DoD have the data base to determine whether the prospective employee or member of the Armed Forces holds such a membership?

Mr. O'Brien. We do not hold a data base, per se. We conduct an extensive investigation. During the interview portion of the investigation, we will ask questions with respect to the person's involvement in activities that might advocate the overthrow of the government or that might advocate the denial of others' constitutional rights. Conceivably the person would have been arrested in some context that might lead to this kind of a discovery.

Mr. Romerstein. But you don't collect data on such organizations so that you would be able to determine if a member of such a group——

Mr. O'Brien. We do not.

Mr. Romerstein. Where would you get that kind of information normally? Is there another agency that would supply it if they had the data?

Mr. O'Donnell. We would go to the Federal Bureau of Investigation and inquire as to their knowledge of the organization.

Mr. Romerstein. If a group such as one of those referred to in Executive Order 10450 publishes a plan to penetrate the armed forces, from whom would you expect to get the information so that you could take protective measures to prevent such people from coming in?

Mr. O'Brien. Our primary source of information of this type is the Federal Bureau of Investigation.

Mr. Romerstein. Thank you.

Donald Perrine and Paul Nugent testified on behalf of the Federal Bureau of Investigation in response to a series of questions by Congressman C. W. (Bill) Young. They testified as follows:

Mr. Young. Mr. Perrine, let me just ask the questions and then anyone, you or anyone can respond.

Mr. Perrine. All right, very well.

Mr. Young. I want to talk about the organizational cases. It is my understanding that most of them have been closed since the Attorney General's guidelines were issued. Is that correct?

Mr. Perrine. Yes, and I would like to have Mr. Nugent address that question more specifically.

Mr. Nugent. The answer to your question is yes, that the majority of the cases, investigative cases which have been closed since the adoption of the guidelines in April 1976 have been due to the criteria established by the guidelines for investigation. They either did not meet that criteria or were closed for another reasons, but the vast majority of them have been closed for that reason.

Mr. Young. Now, if a case on an organization has been closed, is the FBI still permitted to collect public type information relative to the group and its activities?

Mr. Nugent. No, sir.

Mr. Young. You are not.

Mr. Nugent. As a matter of policy, and there is documentation of this, the Department of Justice has considered the collection of public source information or information from the publication of even the group itself which has since been closed as active investigation. Now, that is not to say that certain information on this type which may be volunteering by citizens or other individual sources or informants cannot be accepted in the file.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Mr. YOUNG. What about the case of, say, a newspaper article.
Mr. NUGENT. Yes, sir.
Mr. YOUNG. Are you permitted to collect that?
Mr. NUGENT. To persue the newspaper and clip it? No. sir, that is not done at this point.
Mr. YOUNG. You say it is not done. Are you not permitted to do it?
Mr. NUGENT. I say based on the Department ruling and that one investigative case which was cited specifically by the Department, we would not do that, and do not do that.
Mr. YOUNG. Are you allowed to read it and remember it?
Mr. NUGENT. I would think that might be allowable in the private confines of one's home.

* * * * * *

Mr. YOUNG. When was the case on the Progressive Labor Party Closed?
Mr. NUGENT. The Progressive Labor Party case was closed in September 1976, September 20, 1976, to be exact.
Mr. YOUNG. Well, the Progressive Labor Party has publicly proclaimed that they intend to take power in the United States by using "armed struggle" and that they are engaged in a program of penerating the Armed Forces.
This information appeared in the Progressive Labor Magazine, their own magazine that was published in the spring of 1978.
In a case like this where they themselves have made this declaration, can the FBI collect these public documents on a group like the Progressive Labor Party, despite the fact that the case has been closed?
Mr. NUGENT. Absolutely not.
Mr. YOUNG. Absolutely not.
Now, let me make sure that I make sure I understand and anybody who reads this record understands. The Progressive Labor Party who has proclaimed through their own publication that they edit, publish, print, and somebody pays for, has said that they intend to take power by armed struggle. Now, there is something in gut law against advocating the violent overthrow of the government, isn't there?
Mr. NUGENT. That is quite true. However, due to the nature of the investigations which are conducted under the Domestic Security criteria today, if you have seen the guidelines, it is very specific in that advocacy or rhetoric is not the criteria on which we can base a domestic security investigation. There has to be that one step further, involvement in force and violence and violation of federal law, or at least a conspiracy to violate some federal law with force and violence on which we can base basically a criminal type approach to an investigation, not a searching for programs which groups may advocate in the press or in speechmaking and so forth.
Mr. YOUNG. In other words, you are not allowed to be involved in fire prevention; you have to wait until the fire starts.
Mr. NUGENT. Pretty close to that, yes, sir.
Mr. YOUNG. I wonder what the American people would say if they all knew about that. I have an idea what their reaction would be.
If the United States Army sent you a name in a national agency check of someone who had recently joined the PLP, and had peneteated the Army, which is what they say they are going to do, would you have to answer no record?
Mr. NUGENT. Well, that is a hypothetical question, I realize, and to answer hypotheticals is rather difficult, but if that name were submitted today and that individual had joined such an organization last week, I would say that the possibilities of our coming up with that name in a name check situation would be practically remote.
Mr. YOUNG. Not because you weren't able to do it, but because you weren't permitted to, is that it?
Mr. NUGENT. Well, we just wouldn't have the currency of information with respect to that organization which has been closed now for three years. The membership of that particular group and any other would have changed two times in that period of three years, and we wouldn't have the identities of the membership.
Mr. YOUNG. Since the regulations were issued, have you had any instance of the United States Army giving you a name and asking for information relative to whether or not this person was an infiltrator from the PLO?
Mr. NUGENT. No, sir, we haven't, to my knowledge. Maybe Mr. Perrine could recall one on a name check basis. I don't get involved in the name check process per se.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3

Mr. PERRINE. Mr. Young, the mechanics would be that the Department of Defense or the Army would submit a form, either 1584, one of the routine forms requesting a check of our files. This would be initiating the national agency check. So unless they had some real special reason to flag the organization, we would have no way of knowing beyond our normal search procedure, which would be for any reference in our files, and if the information were not in our files, they would get a no record return.

Mr. YOUNG. But the possibility of that person being what the Army suspected, that he was one of the PLO's infiltrators——

Mr. PERRINE. Would go undetected.

Mr. YOUNG. That worries me. Does that worry you?

Mr. PERRINE. Certainly.

Mr. Young. Well, I am certainly glad it worries more than just me.

There has been previous testimony before this Committee that the FBI closed the case on the Maryland Ku Klux Klan shortly before Maryland State Police arrested a number of the leaders of the group in a plot to bomb churches, Jewish temples and the home of a Member of Congress.

If the State Police had not had Sergeant John Cook under cover in this violent group, they very likely would have been able to bring off this act of terrorism.

Now, if someone had joined the Maryland Klan after you closed that case, and had then applied for security clearance, would you have had any information to supply in a national agency check?

Mr. PERRINE. Probably not unless it came from other sources, another investigative service who may have forwarded it to our agency, but as an active investigation on the part of the FBI, as Mr. Nugent indicated, no.

○

Declassified in Part - Sanitized Copy Approved for Release 2013/01/10 : CIA-RDP90-00530R000500970003-3